



CVE-2016-7797

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2016-7797
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-24 15:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	Pacemaker before 1.1.15, when using pacemaker remote, might allow remote attackers to cause a denial of service (node c

Risk And Classification

Problem Types: CWE-254

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Pacemaker	All	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse	Leap	42.2	All	All	All
Operating System	Opensuse Project	Leap	42.1	All	All	All
Operating System	Opensuse Project	Leap	42.1	All	All	All
Operating System	Redhat	Enterprise Linux High Availability	7.0	All	All	All
Operating System	Redhat	Enterprise Linux High Availability	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Resilient Storage	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Resilient Storage	7.0	All	All	All
Operating System	Suse	Linux Enterprise High Availability	12	sp2	All	All
Operating System	Suse	Linux Enterprise High Availability	12	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	12	sp2	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2016:2965-1: important: Security update	SUSE	lists.opensuse.org

openSUSE-SU-2016:3101-1: moderate: Security update for pacemaker	SUSE	lists.opensuse.org
oss-security - Re: CVE request: pacemaker DoS when pacemaker remote is in use	MLIST	www.opensuse.org
Pacemaker CVE-2016-7797 Remote Denial of Service Vulnerability	BID	www.securityfocus.com
Red Hat Customer Portal	REDHAT	rhn.redhat.com
[security-announce] SUSE-SU-2016:2869-1: important: Security update for	SUSE	lists.opensuse.org
Fix: remote: cl#5269 - Notify other clients of a new connection only ... · ClusterLabs/pacemaker@5ec24a2 · GitHub	CONFIRM	github.com
Bug 5269 – DoS: valid authkey should be required for takeover of a Pacemaker remote	CONFIRM	bugs.clusterlabs.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)